Appendix A
Definitions

Access Approval Authority. Individual responsible for final access approval and/or denial determination.

Access Roster. A database or listing of individuals briefed to a special access program.

Access Termination. The removal of an individual from access to SAP or other Program information.

Accrediting Authority. A Customer official who has the authority to decide on accepting the security safeguards prescribed or who is responsible for issuing an accreditation statement that records the decision to acccept those safeguards.

Acknowledged Special Access Program. A SAP whose existence is publicly acknowledged.

Acquisition Special Access Program (AQ-SAP). A special access program established primarily to protect sensitive research, development, testing, and evaluation (RDT&E) or procurement activities in support of sensitive military and intelligence requirements.

Agent of the Government. A contractor employee designated in writing by the Government Contracting Officer who is authorized to act on behalf of the Government.

Authentication. a. To establish the validity of a claimed identity. b. To provide protection against fraudulent transactions by establishing the validity of message, station, individual, or originator.

Automated Information System (AIS). A generic term applied to all electronic computing systems. AISS are composed of computer hardware (i.e., automated data processing (ADP) equipment and associated devices that may include communication equipment), firmware, operating systems, and other applicable software. AISS collect, store, process, create, disseminate, communicate, or control data or information.

Billets. A determination that in order to meet need-to-know criteria, certain SAPS may elect to limit access to a predetermined number of properly cleared employees. Security personnel do not count against the billet system.

Boundary. The boundary of an AIS or network includes all users that are directly or indirectly connected and who can receive data from the system without a reliable human review by an appropriately cleared authority.

Certification. A statement to an accrediting authority of the extent to which an AIS or network meets its security criteria. This statement is made as part of and in support of the accreditation process.

Clearing. The removal of information from the media to facilitate continued use and to prevent the AIS system from recovering previously stored data. However, the data may be recovered using laboratory techniques. Overwriting and degaussing are acceptable methods of clearing media.

Codeword. A single classified word assigned to represent a specific SAP or portions thereof.

Collateral Information. Collateral information is National Security Information created in parallel with Special Access Information under the Provisions of E.O. 12356 (et al) but which is not subject to the added formal security protection required for Special Access Information (stricter access controls, need-to-know, compartmentation, stricter physical security standards, etc).

Compelling Need. A requirement for immediate access to special program information to prevent failure of the mission or operation or other cogent reasons.

Contractor Program Security Officer (CPSO). An individual appointed by the contractor who performs the security duties and functions for Special Access Programs.

Contractor Program Manager (CPM). A contractor-designated individual who has overall responsibility for all aspects of a Program.

Counterintelligence Awareness. A state of being aware of the sensitivity of classified information one possesses, collaterally aware of the many modes of operation of hostile intelligence persons and others whose interests are inimical to the United States while

being able to recognize attempts to compromise one's information, and the actions one should take, when one suspects he has been approached, to impart the necessary facts to trained counterintelligence personnel.

Customer. The Government organization that sponsors the processing.

Data Integrity. a. The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction. b. The property that data has not been exposed to accidental or malicious alteration or destruction.

Debriefing. The process of informing a person his need-to-know for access is terminated.

Declassification {Media). An administrative step that the owner of the media takes when the classification is lowered to UNCLASSIFIED. The media must be properly sanitized before it can be downgraded to UNCLASSIFIED.

Degauss. a. To reduce the magnetization to zero by applying a reverse (coercive) magnetizing force, commonly referred to as demagnetizing, or b. To reduce the correlation between previous and present data to a point that there is no known technique for recovery of the previous data.

Degausser. An electrical device or hand-held permanent magnet assembly that generates a coercive magnetic force for degaussing magnetic storage media or other magnetic material.

Degaussing (Demagnetizing). Procedure using an approved device to reduce the magnetization of a magnetic storage media to zero by applying a reverse (coercive) magnetizing force rendering any previously stored data unreadable and unintelligible.

Digraph and/or Trigraph. A two and/or three-letter acronym for the assigned Codeword or nickname.

Disclosure Record. A record of names and dates of initial access to any Program information.

e.g. For example (exempli gratia).

Eligibility. A determination that a person meets personnel security standards for access to Program material.

EPROM. A field-programmable read-only memory that can have the data content of each memory cell altered more than once. An EPROM is bulk-erased by exposure to a high-intensity ultraviolet light. Sometimes referred to as a reprogrammable read-only memory.

EEPROM. Abbreviation for electrically erasable programmable read-only memory. These devices are fabricated in much the same way as EPROMs and, therefore, benefit from the industry's accumulated quality and reliability experience. As the name implies, erasure is accomplished by introducing electrical signals in the form of pulses to the device, rather than by exposing the device to ultraviolet light. Similar products using a nitride NMOS process are termed EAROMS (for electrically alterable read-only memory).

Government Program Manager (GPM). The senior Government Program official who has ultimate responsibility for all aspects of the Program.

i.e. That is (id est).

Inadvertent Disclosure. A set of circumstances or a security incident in which a person has had involuntary access to classified information to which the individual was or is not normally authorized.

Indoctrination. An initial indoctrination and/or instruction provided each individual approved to a SAP prior to his exposure concerning the unique nature of Program information and the policies, procedures, and practices for its handling.

Information Systems Security Representative (ISSR). The Provider-assigned individual responsible for the on-site security of the AIS(S) processing information for the Customer.

Joint Use Agreement. A written agreement signed by two or more accrediting authorities whose responsibility includes information processed on a common AIS or network. Such an agreement defines a cognizant security authority and the security arrangements that will govern the operation of the network.

Memorandum of Agreement (MOA). An agreement, the terms of which are delineated and attested to by the signatories thereto. MOA & MOU (Memorandum of Understanding) are used interchangeably.

Network. A computing environment with more than one independent processor interconnected to permit communications and sharing of resources.

Nicknames. A combination of two separate unclassified words assigned to represent a specific SAP or portion thereof.

Nonvolatile Memory Components. Memory components that do retain data when all power sources are disconnected.

Object Reuse. The reassignment to some subject of a medium (e.g., page frame, disk sector, magnetic tape) that contained one or more objects. To be securely reassigned, such media will contain no residual data from the previously contained object(s).

Office Information System (01S). An 01S is a special purpose AIS oriented to word processing, electronic mail, and other similar office functions. An 01S is normally comprised of one or more central processing units, control units, storage devices, user terminals, and interfaces to connect these components.

Overwrite **(Re-recording) Verification.** An approved procedure to review, display, or check the success of an overwrite procedure, or b. The successful testing and documentation through hardware and random hard-copy readout of the actual overwritten memory sectors.

Perimeter. The perimeter of an AIS or network is the extent of the system that is to be accredited as a single system.

Peripheral Devices. Any device attached to the network that can store, print, display, or enhance data (e.g., disk and/or tape, printer and/or plotter, an optical scanner, a video camera, a punched-card reader, a monitor, or card punch).

Personal Computer System (PC). A PC is a system based on a microprocessor and comprised of internal memory (ROMs and RAMs), input and/or output, and associated circuitry. It typically includes one or more read/write device(s) for removable magnetic storage media (e.g., floppy diskettes, tape cassettes, hard disk cartridges), a keyboard, CRT or plasma display, and a printer. It is easily transported and is primarily used on desk tops for word processing, database management, or engineering analysis applications.

Program Access Request (PAR). A formal request used to nominate an individual for Program access.

Program Channels or Program Security Channels. A method or means expressly authorized for the handling or transmission of classified or unclassified SAP information whereby the information is provided to indoctrinated persons.

Program Executive Agent. The highest ranking military or civilian individual charged with direct responsibility for the Program and usually appoints the Government Program Manager.

Program Material. Program material and information describing the service(s) provided, the capabilities developed, or the item(s) produced under the SAP.

Program Security Officer (PSO). The Government official who administers the security policies for the SAP

Program Sensitive Information. Unclassified information that is associated with the Program. Material or information **that,** while not directly describing the Program or aspects of the Program, could indirectly disclose the actual nature of the Program to a non-Program-briefed individual.

Provider. The Contractor or Government-support organization (or both) that provides the process on behalf of the Customer.

Sanitizing. The removal of information from the media or equipment such that data recovery using any known technique or analysis is prevented. Sanitizing shall include the removal of data from the media, as well as the removal of all classified labels, markings, and activity logs. Properly sanitized media may be subsequently declassified upon observing the organization's respective verification and review procedures.

Secure Working Area. An accredited facility or area that is used for handling, discussing and/or processing, but not storage of SAP information.

Security level. A clearance or classification and a set of designators of special access approvals; i.e., a clearance and a set of designators of special access approval or a classification and a set of such designators, the former applying to a user, the latter applying, for example, to a computer object.

Security **Policy.** The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. A complete security policy will necessarily address many concerns beyond the scope of computers and communications.

Security Profile. The approved aggregate of hardware/ software and administrative controls used to protect the system.

Security Testing. A process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed application environment. This process includes hands-on functional testing, penetration testing, and verification. See also: Functional Testing, Penetration Testing, Verification.

Sensitivity Label. A collection of information that represents the security level of an object and that describes the sensitivity of the data in the object. A sensitivity label consists of a sensitivity level (classification and compartments) and other required security markings (e.g., Codewords, handling caveats) to be used for labeling data.

Sensitive Activities. Sensitive activities are special access or Codeword programs, critical research and development efforts, operations or intelligence activities, special plans, special activities, or sensitive support to the customer or customer contractors or clients.

Sensitive Compartmented Information (SCI). SCI is classified information concerning or derived from intelligence sources and methods or analytical processes that is required to be handled within a formal control system established by Director of Central Intelligence.

Sensitive Compartmented Information Facility (SCIF). SCIF is an area, room(s), building installation that is accredited to store, use, discuss, or electronically process Sensitive Compartmented Information (SCI). The standards and procedures for a SCIF are stated in DCIDs 1/19 and 1/21.

Special Access Program Facility (SAPF). A specific physical space that has been formally accredited in writing by the cognizant PSO which satisfies the criteria for generating, safeguarding, handling, discussing, and storing CLASSIFIED and/or UNCLASSIFIED Program information, hardware, and materials.

Special **Program Document Control Center. The** component's activity assigned responsibility by the ISSR for the management, control, and accounting of all documents and magnetic media received or generated as a result of the special program activity.

Stand-Alone AIS. A stand-alone AIS may include desktop, laptop, and notebook personal computers, and any other hand-held electronic device containing classified information. Stand-alone AISS by definition are *not* connected to any LAN or other type of network.

System. An assembly of computer and/or communications hardware, software, and firmware configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting and receiving, storing, and retrieving data with a minimum of human intervention.

Trigraph. (See Digraph ruder Trigraph.)

Trojan Horse. A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security (for example, making a "blind copy" of a sensitive file for the creator of the Trojan horse).

Trusted Computer System. A system that employs sufficient hardware and software integrity measures to allow its use for processing simultaneously a range of sensitive or classified information.

Trusted Path. A mechanism by which a person at a terminal can communicate directly with the trusted computing base. This mechanism can **only be activated by** the person or the trusted computing base and cannot be imitated by untrusted software.

Two-Person Integrity. A provision that prohibits one person from working alone.

Unacknowledged Special Access Program. A SAP with protective controls that ensures the existence of the Program is not acknowledged, affirmed, or made known to any person not authorized for such information. All aspects (e.g., technical, operational, logistical, etc.) are handled in an unacknowledged manner.

Users. Any person who interacts directly with an AIS or a network system. This includes both those persons who are authorized to interact with the system and those people who interact without authorization (e.g., active or passive wiretappers).

Vendor. The manufacturer or sellers of the AIS equipment and/or software used on the special program.

Virus. Malicious software. A form of Trojan horse that reproduces itself in other executable code.

Volatile Memory Components. Memory components that *do not* ***retain*** data after removal of all electrical power sources and when reinserted into a similarly configured AIS do not contain residual data.

Workstation. A high-performance, microprocessor-based platform that uses specialized software applicable to the work environment.